

Web Images Maps News Shopping Gmail more ▾

Sign in

Google

(ibe OR "identity based encryption") AND (multiple authorities)

Search

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

Web Results 1 - 10 of about 63,200 for (ibe OR "identity based encryption") AND (multiple authorities). (0.7)

[PDF] [Fuzzy Identity-Based Encryption](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

create a Fuzzy IBE scheme where the attributes come from multiple authorities. While, it is natural for one authority to certify all attributes that ...

[eprint.iacr.org/2004/086.pdf](http://eprint.iacr.org/2004/086.pdf) - [Similar pages](#)

[PDF] [cs/0703106v1](http://arXiv.org/abs/cs/0703106v1) [cs ...]

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Practical Identity-Based Encryption (IBE) in Multiple ... of a trusted authority (called private key generation, or PKG for short). This eliminates ...

[export.arxiv.org/pdf/cs/0703106](http://export.arxiv.org/pdf/cs/0703106) - [Similar pages](#)

[PDF] [Identity Based Encryption Scheme based on Quadratic Residues](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

for example) and the use of multiple authorities will be desirable. .... D Boneh, M Franklin Identity-Based Encryption from the Weil Pairing Advances ...

[www.cesg.gov.uk/site/ast/idpkc/media/ciren.pdf](http://www.cesg.gov.uk/site/ast/idpkc/media/ciren.pdf) - [Similar pages](#)

[LNCS 3494 - Fuzzy Identity-Based Encryption](#)

it is possible to create a Fuzzy IBE scheme where the attributes come from. multiple authorities. While, it is natural for one authority to certify all ...

[www.springerlink.com/index/k0vd9xqjq4jyyp9m.pdf](http://www.springerlink.com/index/k0vd9xqjq4jyyp9m.pdf) - [Similar pages](#)

[PDF] [IBE Applied to Privacy and Identity Mangement](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Multiple trust authorities [16] can be used, when required, for risk mitiga-. tion. Figure 1 shows the IBE interaction model: ...

[www.hpl.hp.com/techreports/2003/HPL-2003-101.pdf](http://www.hpl.hp.com/techreports/2003/HPL-2003-101.pdf) - [Similar pages](#)

[A flexible role-based secure messaging service: exploiting ibe ...](#)

include multiple trust authorities, run by independent. authorities, in order to avoid the ...

[7] C. Cocks, An Identity Based Encryption Scheme based on ...

[ieeexplore.ieee.org/iel5/6719/27592/01232060.pdf](http://ieeexplore.ieee.org/iel5/6719/27592/01232060.pdf) - [Similar pages](#)

[PDF] [An Identity Based Encryption Scheme based on Quadratic Residues](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

An Identity Based Encryption Scheme based on Quadratic Residues. Overview .....

Authority fully trusted. • Or multiple authorities used (Multi Party ...

[www.crypto.ethz.ch/teaching/lectures/ISS06/slides/Saner-Celebi.pdf](http://www.crypto.ethz.ch/teaching/lectures/ISS06/slides/Saner-Celebi.pdf) - [Similar pages](#)

[Patroklos Argyroudís / Identity-based encryption resources](#)

related to identity-based encryption (IBE) (or identity-based cryptography ... Applications of Multiple Trust Authorities in Pairing Based Cryptosystems ...

[ntrg.cs.tcd.ie/~argp/ibe.html](http://ntrg.cs.tcd.ie/~argp/ibe.html) - 13k - [Cached](#) - [Similar pages](#)

[Identity-based encryption system - US Patent 6886096](#)

A system is provided that uses identity-based encryption to support secure ... the system further comprises a certification authority through which at least ...

[www.patentstorm.us/patents/6886096-claims.html](http://www.patentstorm.us/patents/6886096-claims.html) - 26k - [Cached](#) - [Similar pages](#)

### Multiple Trusted Authorities in Identifier Based Cryptography from ...

Our solution makes use of Multiple Trusted Authorities in Identifier Based ... 2: An identity based encryption scheme based on quadratic residues (context) ...  
citeseer.ist.psu.edu/chen03multiple.html - 28k - [Cached](#) - [Similar pages](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

---

(ibe OR "identity based encryption") AND (multiple authorities)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#) | [Try Google Experimental](#)

---

©2008 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

[Web](#) [Images](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more ▾](#)[Sign in](#)**Google**

multiple identities identity based encryption

**Search**[Advanced Search](#)  
[Preferences](#)**Web** Results 1 - 10 of about 1,670,000 for multiple identities identity based encryption. (0.29 seconds)**[PDF] Practical Identity-Based Encryption (IBE) in Multiple-PKG ...**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Identity-based encryption (IBE) schemes are usually used in multiple- PKG environments — on the one hand, each administrative domain (e.g., a ...

[eprint.iacr.org/2007/100.pdf](http://eprint.iacr.org/2007/100.pdf) - [Similar pages](#)**[PDF] Fuzzy Identity-Based Encryption**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Identity-Based Encryption. In Fuzzy IBE we view an identity as set of .... the identity any IBE scheme that encrypts to multiple attributes must provide ...

[eprint.iacr.org/2004/086.pdf](http://eprint.iacr.org/2004/086.pdf) - [Similar pages](#)[More results from eprint.iacr.org »](#)**[cs/0703106] Practical Identity-Based Encryption (IBE) in Multiple ...**

Title: Practical Identity-Based Encryption (IBE) in Multiple PKG Environments and Its Applications. Authors: Shengbao Wang. (Submitted on 22 Mar 2007) ...

[arxiv.org/abs/cs/0703106](http://arxiv.org/abs/cs/0703106) - 6k - [Cached](#) - [Similar pages](#)**Identity Based Encryption Without Redundancy**

proposed multiple-recipient IBE scheme. Our modification of the latter ... Finding a practical identity based encryption scheme (IBE) remained an ...

[www.springerlink.com/index/YLWHMJWLLTBU06DH.pdf](http://www.springerlink.com/index/YLWHMJWLLTBU06DH.pdf) - [Similar pages](#)**[PDF] Identity Based Encryption Scheme based on Quadratic Residues**File Format: PDF/Adobe Acrobat - [View as HTML](#)

C Cocks Split Generation of RSA Parameters with Multiple Participants Proceed- ... D

Boneh, M Franklin Identity-Based Encryption from the Weil Pairing ...

[www.cesg.gov.uk/site/ast/idpko/media/ciren.pdf](http://www.cesg.gov.uk/site/ast/idpko/media/ciren.pdf) - [Similar pages](#)**About Voltage**

Apr 4, 2006 ... Voltage Security's Identity-Based Encryption ... Easy to use – no need for end users to worry about keys, certificates or multiple inboxes. ...

[www.voltage.com/about/pressreleases/PR060404.htm](http://www.voltage.com/about/pressreleases/PR060404.htm) - 17k - [Cached](#) - [Similar pages](#)**Thoughts on Identity Based Encryption**

May 18, 2005 ... Thoughts on Identity Based Encryption. Your Full Name:. Your Email Address:. Recipient Email(s): Separate multiple addresses with commas. ...

[blogs.ittoolbox.com/eai/leadership/archives/thoughts-on-identity-based-encryption-4235](http://blogs.ittoolbox.com/eai/leadership/archives/thoughts-on-identity-based-encryption-4235) - 80k - [Cached](#) - [Similar pages](#)**[PDF] Simple Identity-Based Cryptography with Mediated RSA**File Format: PDF/Adobe Acrobat - [View as HTML](#)

The main feature of identity-based encryption is the sender's ability to encrypt ... We stress that using the same modulus by multiple users in a normal RSA ...

[www.isi.edu/divisions/div7/publication\\_files/rsa.pdf](http://www.isi.edu/divisions/div7/publication_files/rsa.pdf) - [Similar pages](#)**Patroklos Argyroudis / Identity-based encryption resources**

Identity Based Encryption from the Tate Pairing to Secure Email Communications: M. Baldwin. ... Applications of Multiple Trust Authorities in Pairing Based ...

[ntrg.cs.tcd.ie/~argp/ibe.html](http://ntrg.cs.tcd.ie/~argp/ibe.html) - 13k - [Cached](#) - [Similar pages](#)

Proofpoint adds Voltage's identity-based encryption to appliance ...  
Apr 11, 2007 ... Proofpoint adds Voltage's identity-based encryption to appliance ...  
(Comma separation for multiple addresses). Your Message: ...  
[www.networkworld.com/news/2007/041107-proofpoint-voltage-encryption.html](http://www.networkworld.com/news/2007/041107-proofpoint-voltage-encryption.html) - 83k -  
[Cached](#) - [Similar pages](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

---

multiple identities identity based encryption

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#) | [Try Google Experimental](#)

---

©2008 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

Web Images Maps News Shopping Gmail more ▾

[Sign in](#)

Google

multiple identities identity based encryption

Search

[Advanced Search](#)  
[Preferences](#)

Web Results 11 - 20 of about 1,670,000 for multiple identities identity based encryption. (0.21 seconds)

[PDF] [Efficient Multi-Receiver Identity-Based Encryption and Its ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

To our knowledge, identity-based encryption in the multi-receiver setting has not been ...

Encryption algorithm Encrypt: Providing multiple identities (ID ...

[www1.i2r.a-star.edu.sg/~jsbaek/publications/emrbe\\_pkc05.pdf](http://www1.i2r.a-star.edu.sg/~jsbaek/publications/emrbe_pkc05.pdf) - [Similar pages](#)

[Jon Udell: Voltage Security's identity-based encryption](#)

Anyway, the real benefit of identity-based encryption, according to Voltage .... Matrox -

Bring multiple monitors to existing notebook and desktop systems. ...

[weblog.infoworld.com/udell/2003/07/08.html](http://weblog.infoworld.com/udell/2003/07/08.html) - 50k - [Cached](#) - [Similar pages](#)

[PDF] [<a href="http://arXiv.org/abs/cs/0703106v1">arXiv:cs/0703106v1 \[cs ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Mar 22, 2007 ... Practical Identity-Based Encryption (IBE) in Multiple. PKG Environments

and Its Applications. Shengbao Wang. Department of Computer Science ...

[export.arxiv.org/pdf/cs/0703106](http://export.arxiv.org/pdf/cs/0703106) - [Similar pages](#)

[Practical Identity-Based Encryption \(IBE\) in Multiple PKG ...](#)

Practical Identity-Based Encryption (IBE) in Multiple PKG Environments and Its

Applications. Authors: Wang, Shengbao. Publication: eprint arXiv:cs/0703106 ...

[adsabs.harvard.edu/abs/2007cs.....3106W](http://adsabs.harvard.edu/abs/2007cs.....3106W) - [Similar pages](#)

[Efficient Multi-receiver Identity-Based Encryption and Its ...](#)

Efficient Multi-receiver Identity-Based Encryption. 383. • Encryption algorithm Encrypt:

Providing multiple identities (ID. 1. ,..., ID. n. ) of the ...

[www.springerlink.com/index/8VCKTDC7PVL0CK4B.pdf](http://www.springerlink.com/index/8VCKTDC7PVL0CK4B.pdf) - [Similar pages](#)

[PS] [ID-Based Encryption for Complex Hierarchies with Applications to ...](#)

File Format: Adobe PostScript - [View as Text](#)

For the same reason, the multiple hierarchical identity-based encryption (MHIBE) scheme

gen-. eralized from Scheme III is not collusion-resistant, ...

[www.cs.brown.edu/~anna/papers/yfd04.ps](http://www.cs.brown.edu/~anna/papers/yfd04.ps) - [Similar pages](#)

[PDF] [Relations Among Notions of Security for Identity Based Encryption ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

challenge identities cannot be made. Definition 5 (Semantic security under multiple-

challenge CCA2). Let IBE = (S, X, E, D) be an identity based encryption ...

[www.cs.ru.nl/paw/publications/latin19a.pdf](http://www.cs.ru.nl/paw/publications/latin19a.pdf) - [Similar pages](#)

[Exploiting Hierarchical Identity-Based Encryption for Access ...](#)

encryption-based access-control architecture that exploits. hierarchical identity-based

encryption in order to deal with. multiple, hierarchical constraints ...

[ieeexplore.ieee.org/iel5/10695/33755/01607594.pdf?](http://ieeexplore.ieee.org/iel5/10695/33755/01607594.pdf?isnumber=33755&prod=CNF&amnumber=1607594&ar...)

[isnumber=33755&prod=CNF&amnumber=1607594&ar...](http://ieeexplore.ieee.org/iel5/10695/33755/01607594.pdf?isnumber=33755&prod=CNF&amnumber=1607594&ar...) - [Similar pages](#)

[PDF] [A Survey of Identity-Based Cryptography](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

cessful realization of identity-based encryption. .... Smart: Applications of Multiple Trust

Author-. ities in Pairing Based Cryptosystems, Proceed- ...

[jan.newmarch.name/publications/auug\\_id\\_survey.pdf](http://jan.newmarch.name/publications/auug_id_survey.pdf) - [Similar pages](#)

### Identity-based encryption system - Patent 6886096

However, if multiple organizations run separate identity-based encryption systems with different master secrets, it may be difficult for users associated ...

[www.freepatentsonline.com/6886096.html](http://www.freepatentsonline.com/6886096.html) - 108k - [Cached](#) - [Similar pages](#)

[Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [Next](#)

---

multiple identities identity based encryption

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Try Google Experimental](#)

---

©2008 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#)

Welcome United States Patent and Trademark Office

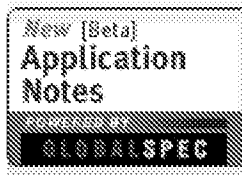
Search Results

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "((bilinear &lt;and&gt; encrypt)&lt;in&gt;metadata)"

Your search matched 4 of 1768462 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[Search Options](#)[View Session History](#)[New Search](#)

» Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

Modify Search

((bilinear &lt;and&gt; encrypt)&lt;in&gt;metadata)

☐ Check to search only within this results set

Display Format:



Citation



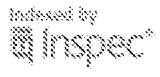
Citation &amp; Abstract

[IEEE/ET](#)[Books](#)[Educational Courses](#)

IEEE/ET journals, transactions, letters, magazines, conference proceedings, and standards.

**view selected items**[Select All](#) [Deselect All](#)

1. Multi-Dimensional Range Query over Encrypted Data  
Shi, Elaine; Bethencourt, John; Chan, T-H. Hubert; Song, Dawn; Perrig, Adrian;  
[Security and Privacy, 2007. SP '07. IEEE Symposium on](#)  
20-23 May 2007 Page(s):350 - 364  
Digital Object Identifier 10.1109/SP.2007.29  
[AbstractPlus](#) | Full Text: [PDF](#)(309 KB) IEEE CNF  
[Rights and Permissions](#)
2. An ID-based broadcast encryption scheme for key distribution  
Xinjun Du; Ying Wang; Jianhua Ge; Yumin Wang;  
[Broadcasting, IEEE Transactions on](#)  
Volume 51, Issue 2, June 2005 Page(s):264 - 266  
Digital Object Identifier 10.1109/TBC.2005.847600  
[AbstractPlus](#) | [References](#) | Full Text: [PDF](#)(120 KB) IEEE JNL  
[Rights and Permissions](#)
3. Low-cost Anonymous Timed-Release Encryption  
Hristu-Varsakelis, D.; Chalkias, K.; Stephanides, G.;  
[Information Assurance and Security, 2007. IAS 2007. Third International Symposium on](#)  
29-31 Aug. 2007 Page(s):77 - 82  
Digital Object Identifier 10.1109/ISIAS.2007.4299754  
[AbstractPlus](#) | Full Text: [PDF](#)(158 KB) IEEE CNF  
[Rights and Permissions](#)
4. Multi-receiver Certificate-Based Encryption and Application to Public Key Broadcast Encry  
Sur, Chul; Jung, Chae Duk; Rhee, Kyung Hyune;  
[Bio-inspired, Learning, and intelligent Systems for Security, 2007. BLISS 2007. ECSIS Symposiu](#)  
9-10 Aug. 2007 Page(s):35 - 40  
Digital Object Identifier 10.1109/BLISS.2007.32  
[AbstractPlus](#) | Full Text: [PDF](#)(251 KB) IEEE CNF  
[Rights and Permissions](#)



[Help](#) [Contact](#)

[Copy](#)




[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase His](#)

Welcome United States Patent and Trademark Office

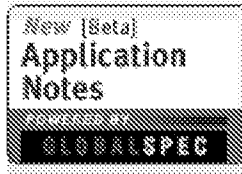
Search Results

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "((bilinear &lt;and&gt; public)&lt;in&gt;metadata)"

Your search matched 38 of 1768462 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.



» Search Options

[View Session History](#)[New Search](#)

» Key

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

Modify Search

((bilinear &lt;and&gt; public)&lt;in&gt;metadata)

[Search](#) »☐ Check to search only within this results set

Display Format:



Citation



Citation &amp; Abstract

[IEEE/ET](#)[Books](#)[Educational Courses](#)

IEEE/ET journals, transactions, letters, magazines, conference proceedings, and standards.

[view selected items](#)[Select All](#) [Deselect All](#)

1. A Method for Fast Revocation of Certificateless Public Key Cryptography  
 Ibrahim, I.I.; Ibrahim, M.H.; Allam, A.M.;  
[Computer Engineering and Systems, The 2006 International Conference on](#)  
 5-7 Nov. 2006 Page(s):250 - 253  
 Digital Object Identifier 10.1109/ICCES.2006.320456  
[AbstractPlus](#) | Full Text: [PDF\(3972 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
2. A New Blind Identity-Based Signature Scheme  
 Elkamchouchi, H.; Abouelseoud, Y.;  
[Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE](#)  
 10-12 Jan. 2008 Page(s):1102 - 1106  
 Digital Object Identifier 10.1109/ccnc08.2007.249  
[AbstractPlus](#) | Full Text: [PDF\(208 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
3. A new blind identity-based signature scheme  
 Elkamchouchi, H.; Abouelseoud, Y.;  
[Computer Engineering & Systems, 2007. ICCES '07. International Conference on](#)  
 27-29 Nov. 2007 Page(s):114 - 119  
 Digital Object Identifier 10.1109/ICCES.2007.4447035  
[AbstractPlus](#) | Full Text: [PDF\(198 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
4. Two Threshold Multisignature Schemes from Bilinear Pairings  
 Li, Guowen; Yu, Jia; Li, Rupeng; Li, Daxing;  
[Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on](#)  
 April 2007 Page(s):1041 - 1045  
 Digital Object Identifier 10.1109/MUE.2007.210  
[AbstractPlus](#) | Full Text: [PDF\(301 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
5. Identity based KCDSA signcryption  
 Jong-Ho Ryu; Youn-Seo Jeong; Dong-il Seo;

[Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference](#)  
Volume 2, 20-22 Feb. 2006 Page(s):6 pp.

[AbstractPlus](#) | [Full Text: PDF\(432 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



6. Invariant bilinear forms and its application in information security  
Li Gao;

[Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference on](#)  
10-12 Aug. 2005 Page(s):649 - 654  
Digital Object Identifier 10.1109/INDIN.2005.1560453

[AbstractPlus](#) | [Full Text: PDF\(1068 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



7. Identity based threshold proxy signcryption scheme  
Meng Wang; Zhijing Liu;

[Computer and Information Technology, 2005. CIT 2005. The Fifth International Conference on](#)  
21-23 Sept. 2005 Page(s):695 - 699  
Digital Object Identifier 10.1109/CIT.2005.129

[AbstractPlus](#) | [Full Text: PDF\(200 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



8. Identity-based threshold signature scheme from the bilinear pairings (extended abstract)  
Joonsang Baek; Yuliang Zheng;

[Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Co](#)  
Volume 1, 2004 Page(s):124 - 128 Vol. 1  
Digital Object Identifier 10.1109/ITCC.2004.1286437

[AbstractPlus](#) | [Full Text: PDF\(1363 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



9. An Improved Identity-Based KCDsA Signcryption Scheme  
Li, Fagen; Xu, Chunxiang;

[Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on](#)  
1-3 Nov. 2007 Page(s):230 - 232  
Digital Object Identifier 10.1109/ISDPE.2007.46

[AbstractPlus](#) | [Full Text: PDF\(190 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



10. An Efficient ID-Based Partially Blind Signature Scheme  
Hu, Xiaoming; Huang, Shangteng;

[Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007](#)  
[International Conference on](#)  
Volume 3, July 30 2007-Aug. 1 2007 Page(s):291 - 296  
Digital Object Identifier 10.1109/SNPD.2007.146

[AbstractPlus](#) | [Full Text: PDF\(277 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



11. Certificateless Designated Verifier Signature Schemes  
Xinyi Huang; Susilo, W.; Yi Mu; Futai Zhang;

[Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Confere](#)  
Volume 2, 18-20 April 2006 Page(s):15 - 19  
Digital Object Identifier 10.1109/AINA.2006.124

[AbstractPlus](#) | [Full Text: PDF\(232 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



12. ID-based one round authenticated group key agreement protocol with bilinear pairings  
Yijuan Shi; Gongliang Chen; Jianhua Li;

[Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on](#)  
Volume 1, 4-6 April 2005 Page(s):757 - 761 Vol. 1  
Digital Object Identifier 10.1109/ITCC.2005.169

[AbstractPlus](#) | [Full Text: PDF\(94 KB\)](#) [IEEE CNF](#)

[Rights and Permissions](#)

## 13. Identity based proxy-signcryption scheme from pairings

Xiangxue Li; Kefei Chen;

[Services Computing, 2004. \(SCC 2004\). Proceedings, 2004 IEEE International Conference on](#)  
15-18 Sept. 2004 Page(s):494 - 497

Digital Object Identifier 10.1109/SCC.2004.1358050

[AbstractPlus](#) | Full Text: [PDF](#)(257 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 14. ID-based tripartite key agreement protocol with pairings

Shengli Liu; Fangguo Zhang; Kefei Chen;

[Information Theory, 2003. Proceedings. IEEE International Symposium on](#)  
29 June-4 July 2003 Page(s):136

Digital Object Identifier 10.1109/ISIT.2003.1228150

[AbstractPlus](#) | Full Text: [PDF](#)(217 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 15. Public Key Broadcast Encryption Schemes With Shorter Transmissions

Park, J. H.; Kim, H. J.; Sung, M. H.; Lee, D. H.;

[Broadcasting, IEEE Transactions on](#) : Accepted for future publication

Volume PP, Issue 99, 2003 Page(s):1 - 1

Digital Object Identifier 10.1109/TBC.2008.919940

[AbstractPlus](#) | Full Text: [PDF](#)(607 KB) [IEEE JNL](#)

## 16. A Brief Look at Pairings Based Cryptography

Boneh, D.;

[Foundations of Computer Science, 2007. FOCS '07. 48th Annual IEEE Symposium on](#)  
21-23 Oct. 2007 Page(s):19 - 26

Digital Object Identifier 10.1109/FOCS.2007.4389476

[AbstractPlus](#) | Full Text: [PDF](#)(257 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 17. An Identity-Based Threshold Ring Signature Scheme Based on the Bilinear Pairings

Shang, Jiu-Qing; Xu, Qiu-Liang; Liu, Xin;

[Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on](#)  
1-3 Nov. 2007 Page(s):233 - 235

Digital Object Identifier 10.1109/ISDPE.2007.44

[AbstractPlus](#) | Full Text: [PDF](#)(285 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 18. A New Dynamic Threshold Secret Sharing Scheme from Bilinear Maps

Wei, Chen; Xiang, Long; Yuebin, Bai; Xiaopeng, Gao;

[Parallel Processing Workshops, 2007. ICPPW 2007. International Conference on](#)  
10-14 Sept. 2007 Page(s):19 - 19

Digital Object Identifier 10.1109/ICPPW.2007.10

[AbstractPlus](#) | Full Text: [PDF](#)(191 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 19. Cryptanalysis and Improvement of a Certificateless Proxy Signature Scheme from Bilinear

Lu, Rongbo; He, Dake; Wang, Changji;

[Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. International Conference on](#)

Volume 3, July 30 2007-Aug. 1 2007 Page(s):285 - 290

Digital Object Identifier 10.1109/SNPD.2007.220

[AbstractPlus](#) | Full Text: [PDF](#)(402 KB) [IEEE CNF](#)[Rights and Permissions](#)

## 20. Two Certificateless Aggregate Signatures From Bilinear Maps

Gong, Zheng; Long, Yu; Hong, Xuan; Chen, Kefei;

[Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. International Conference on](#)

Volume 3, July 30 2007-Aug. 1 2007 Page(s):188 - 193

Digital Object Identifier 10.1109/SNPD.2007.556

[AbstractPlus](#) | [Full Text: PDF\(308 KB\)](#) | [IEEE CNF](#)

[Rights and Permissions](#)



21. Designated Verifier Proxy Signature Scheme from Bilinear Pairings

Rongxing Lu; Zhenfu Cao; Xiaolei Dong; Renwang Su;

[Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums](#)

Volume 2, 20-24 April 2006 Page(s):40 - 47

Digital Object Identifier 10.1109/IMSCCS.2006.211

[AbstractPlus](#) | [Full Text: PDF\(272 KB\)](#) | [IEEE CNF](#)

[Rights and Permissions](#)



22. Identity-based Key Agreement Protocol for Mobile Ad-hoc Networks Using Bilinear Pairing

Hung-Yu Chien; Ru-Yu Lin;

[Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on](#)

Volume 1, 05-07 June 2006 Page(s):520 - 529

[AbstractPlus](#) | [Full Text: PDF\(352 KB\)](#) | [IEEE CNF](#)

[Rights and Permissions](#)



23. Character image reconstruction from a feature space using shape morphing and genetic algorithm

Iga, C.; Wakahara, T.;

[Frontiers in Handwriting Recognition, 2004. IWFHR-9 2004. Ninth International Workshop on](#)

26-29 Oct. 2004 Page(s):341 - 346

Digital Object Identifier 10.1109/IWFHR.2004.25

[AbstractPlus](#) | [Full Text: PDF\(160 KB\)](#) | [IEEE CNF](#)

[Rights and Permissions](#)



24. An efficient finite-field convolution to enhance the performance of the wavelet cryptosystem

Noorkami, M.; Fekri, F.;

[Information Technology, Coding and Computing \[Computers and Communications\], 2003. Process Conference on](#)

28-30 April 2003 Page(s):495 - 499

[AbstractPlus](#) | [Full Text: PDF\(270 KB\)](#) | [IEEE CNF](#)

[Rights and Permissions](#)



25. An ID-based broadcast encryption scheme for key distribution

Xinjun Du; Ying Wang; Jianhua Ge; Yumin Wang;

[Broadcasting, IEEE Transactions on](#)

Volume 51, Issue 2, June 2005 Page(s):264 - 266

Digital Object Identifier 10.1109/TBC.2005.847600

[AbstractPlus](#) | [References](#) | [Full Text: PDF\(120 KB\)](#) | [IEEE JNL](#)

[Rights and Permissions](#)

[Help](#) [Contact](#)

[© Copy](#)

indexed by  
 Inspec®


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#)

Welcome United States Patent and Trademark Office

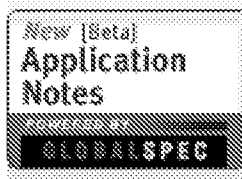
Search Results

[BROWSE](#)
[SEARCH](#)
[IEEE XPLORE GUIDE](#)

Results for "((bilinear &lt;and&gt; mapping)&lt;in&gt;metadata)"

Your search matched 138 of 1768462 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.


[Search Options](#)
[View Session History](#)
[New Search](#)
[Key](#)

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

Modify Search

((bilinear &lt;and&gt; mapping)&lt;in&gt;metadata)

☐ Check to search only within this results set

Display Format:



Citation



Citation &amp; Abstract

IEEE/ET

Books

Educational Courses

IEEE/ET journals, transactions, letters, magazines, conference proceedings, and standards.

[Select All](#) [Deselect All](#)

1. Conformal image warping  
 Frederick, C.; Schwartz, E.L.;  
[Computer Graphics and Applications, IEEE](#)  
 Volume 10, Issue 2, March 1990 Page(s):54 - 61  
 Digital Object Identifier 10.1109/38.50673  
[AbstractPlus](#) | Full Text: [PDF\(1368 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
2. Untraceability of Group Signature Schemes based on Bilinear Mapping and Their Improven  
 Park, Haeryong; Kim, Hyun; Chun, Kilsoo; Lee, Jaeil; Lim, Seongan; Yie, Ikkwon;  
[Information Technology, 2007. ITNG '07. Fourth International Conference on](#)  
 2-4 April 2007 Page(s):747 - 753  
 Digital Object Identifier 10.1109/ITNG.2007.199  
[AbstractPlus](#) | Full Text: [PDF\(308 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
3. Bark and ERB bilinear transforms  
 Smith, J.O., III; Abel, J.S.;  
[Speech and Audio Processing, IEEE Transactions on](#)  
 Volume 7, Issue 6, Nov. 1999 Page(s):697 - 708  
 Digital Object Identifier 10.1109/89.799695  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(352 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
4. Experimental evaluation of the bilinear transformation used in the CT-based attenuation cc  
 imaging  
 Jianhua Yu.; Jurgen Seidel.; Pomper, Martin; Tsui, Benjamin M.W.;  
[Nuclear Science Symposium Conference Record, 2007. NSS '07. IEEE](#)  
 Volume 5, Oct. 26 2007-Nov. 3 2007 Page(s):3747 - 3750  
 Digital Object Identifier 10.1109/NSSMIC.2007.4436937  
[AbstractPlus](#) | Full Text: [PDF\(221 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
5. Optimal MAP estimation of bilinear systems via the EM algorithm  
 Krishnamurthy, V.; Johnston, L.; Logothetis, A.;

- [Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on](#)  
Volume 4, 12-15 May 1998 Page(s):2373 - 2376 vol.4  
Digital Object Identifier 10.1109/ICASSP.1998.681627  
[AbstractPlus](#) | Full Text: [PDF\(300 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
6. Bilinear and 2-power input-output maps: Finite dimensional realizations and the role of fun  
Gilbert, E.;  
[Automatic Control, IEEE Transactions on](#)  
Volume 23, Issue 3, Jun 1978 Page(s):418 - 425  
[AbstractPlus](#) | Full Text: [PDF\(784 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
7. Shift operators and bilinear system theory  
Frazho, A.E.;  
[Decision and Control including the 17th Symposium on Adaptive Processes, 1978 IEEE Conference on](#)  
Volume 17, Part 1, Jan. 1978 Page(s):551 - 556  
Digital Object Identifier 10.1109/CDC.1978.267991  
[AbstractPlus](#) | Full Text: [PDF\(502 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
8. Finite dimensional smoothers for MAP state estimation of bilinear systems  
Johnston, L.A.; Krishnamurthy, V.;  
[Signal Processing, IEEE Transactions on \[see also Acoustics, Speech, and Signal Processing, IE](#)  
Volume 47, Issue 9, Sept. 1999 Page(s):2444 - 2459  
Digital Object Identifier 10.1109/78.782188  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(428 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
9. Continuous-time to discrete-time conversion via a novel parametrized s-to-z-plane mappin  
Melvin, W.L.; Frey, D.R.;  
[Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on \[see also Ci](#)  
[Briefs, IEEE Transactions on\]](#)  
Volume 44, Issue 10, Oct. 1997 Page(s):829 - 834  
Digital Object Identifier 10.1109/82.633441  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(200 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
10. Analysis of recursive MAP algorithm for state estimation of bilinear systems  
Krishnamurthy, V.; Yin, G.;  
[Decision and Control, 2000. Proceedings of the 39th IEEE Conference on](#)  
Volume 4, 12-15 Dec. 2000 Page(s):3799 - 3800 vol.4  
Digital Object Identifier 10.1109/CDC.2000.912302  
[AbstractPlus](#) | Full Text: [PDF\(160 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
11. Hardware support for floating point map function generation  
O'Grady, E.P.;  
[Simulation Symposium, 1999. Proceedings. 32nd Annual](#)  
11-15 April 1999 Page(s):145 - 152  
Digital Object Identifier 10.1109/SIMSYM.1999.766466  
[AbstractPlus](#) | Full Text: [PDF\(84 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
12. The Bark bilinear transform  
Smith, J.O., III; Abel, J.S.;  
[Applications of Signal Processing to Audio and Acoustics, 1995., IEEE ASSP Workshop on](#)  
15-18 Oct. 1995 Page(s):202 - 205  
Digital Object Identifier 10.1109/ASPAA.1995.482991  
[AbstractPlus](#) | Full Text: [PDF\(316 KB\)](#) [IEEE CNF](#)

[Rights and Permissions](#)

13. Mapping and pseudoinverse algorithms for ocean data assimilation  
Fieguth, P.W.; Menemenlis, D.; Fukumori, I.;  
[Geoscience and Remote Sensing, IEEE Transactions on](#)  
Volume 41, *Issue 1*, Jan. 2003 Page(s):43 - 51  
Digital Object Identifier 10.1109/TGRS.2002.808058  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(731 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
14. Computational aspects of the bilinear transformation based algorithm for S-plane to Z-plane  
Krishna, H.;  
[Automatic Control, IEEE Transactions on](#)  
Volume 33, *Issue 11*, Nov. 1988 Page(s):1086 - 1088  
Digital Object Identifier 10.1109/9.14427  
[AbstractPlus](#) | Full Text: [PDF\(240 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
15. Polynomial perceptrons and their applications to fading channel equalization and co-channel interference  
Zengjun Xiang; Guangguo Bi; Tho Le-Ngoc;  
[Signal Processing, IEEE Transactions on \[see also Acoustics, Speech, and Signal Processing, IEEE Transactions on\]](#)  
Volume 42, *Issue 9*, Sept. 1994 Page(s):2470 - 2480  
Digital Object Identifier 10.1109/78.317868  
[AbstractPlus](#) | Full Text: [PDF\(772 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
16. Fault diagnosis in electronic circuits based on bilinear transformation in 3-D and 4-D space  
Czaja, Z.; Zielonko, R.;  
[Instrumentation and Measurement, IEEE Transactions on](#)  
Volume 52, *Issue 1*, Feb. 2003 Page(s):97 - 102  
Digital Object Identifier 10.1109/TIM.2003.809075  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(546 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
17. Time-Width Versus Frequency Band Mapping of Energy Distributions  
Umapathy, K.; Krishnan, S.;  
[Signal Processing, IEEE Transactions on \[see also Acoustics, Speech, and Signal Processing, IEEE Transactions on\]](#)  
Volume 55, *Issue 3*, March 2007 Page(s):978 - 989  
Digital Object Identifier 10.1109/TSP.2006.887131  
[AbstractPlus](#) | Full Text: [PDF\(2090 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)
18. Realization of discrete-time internally bilinear systems  
T. J. Tarn; Nonoyama, S.;  
[Decision and Control including the 15th Symposium on Adaptive Processes, 1976 IEEE Conference on](#)  
Volume 15, Part 1, Dec. 1976 Page(s):125 - 133  
Digital Object Identifier 10.1109/CDC.1976.267715  
[AbstractPlus](#) | Full Text: [PDF\(730 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
19. Graphical Analysis of Transformed Feedback Bilinear Expressions Applied to Differential Algebraic Equations  
Consospo, M.A. Lopez; Gonzalez-Villarruel, J.E.;  
[Electrical and Electronics Engineering, 2007. ICEEE 2007. 4th International Conference on](#)  
5-7 Sept. 2007 Page(s):225 - 228  
Digital Object Identifier 10.1109/ICEEE.2007.4345011  
[AbstractPlus](#) | Full Text: [PDF\(1830 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
20. On the Rationality of the Composition Product: A Survey  
Espinosa, L.A.D.; Gray, W.S.; Gonzalez, O.R.;

[System Theory, 2007. SSST '07. Thirty-Ninth Southeastern Symposium on](#)  
4-6 March 2007 Page(s):238 - 243  
Digital Object Identifier 10.1109/SSST.2007.352356

[AbstractPlus](#) | Full Text: [PDF\(5941 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



21. Some potential pitfalls with s to z-plane mappings  
Harvey, R.; Mandic, D.P.; Kolonic, D.H.;

[Acoustics, Speech, and Signal Processing, 2000. ICASSP '00. Proceedings. 2000 IEEE International Conference on](#)  
Volume 6, 5-9 June 2000 Page(s):3530 - 3533 vol.6  
Digital Object Identifier 10.1109/ICASSP.2000.860163

[AbstractPlus](#) | Full Text: [PDF\(228 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



22. System for non-invasive epicardial potential mapping and impedance tomography  
Shim, U.; Kumarakrishnan, A.; Cahn, S.B.; Sleator, T.;

[Engineering in Medicine and Biology society, 1997. Proceedings of the 19th Annual International Conference on](#)  
Volume 1, 30 Oct.-2 Nov. 1997 Page(s):201  
Digital Object Identifier 10.1109/IEMBS.1997.754542

[AbstractPlus](#) | Full Text: [PDF\(300 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)



23. Direct construction of minimal bilinear realizations from nonlinear input-output maps  
Isidori, A.;

[Automatic Control, IEEE Transactions on](#)  
Volume 18, Issue 6, Dec 1973 Page(s):626 - 631

[AbstractPlus](#) | Full Text: [PDF\(584 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)



24. Bilinear systems with homogeneous input-output maps  
Evans, M.;

[Automatic Control, IEEE Transactions on](#)  
Volume 28, Issue 1, Jan 1983 Page(s):113 - 115

[AbstractPlus](#) | Full Text: [PDF\(288 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)



25. A scheme for reconstructing height of 3D terrain map from shading of a multi-spectral band  
Damrongwatthanayothin, B.; Roeksabutr, A.; Jantarang, S.;

[TENCON 2004, 2004 IEEE Region 10 Conference](#)  
Volume A, 21-24 Nov. 2004 Page(s):411 - 414 Vol. 1  
Digital Object Identifier 10.1109/TENCON.2004.1414444

[AbstractPlus](#) | Full Text: [PDF\(1969 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

V

[Help](#) [Contact](#)

[© Copy](#)

Indexed by  
 Inspec®




[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#)

Welcome United States Patent and Trademark Office

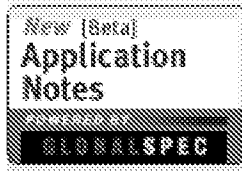
Search Results

[BROWSE](#)
[SEARCH](#)
[IEEE XPLORE GUIDE](#)

Results for "((bilinear &lt;and&gt; authorities)&lt;in&gt;metadata)"

Your search matched 5 of 1768462 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.


[» Search Options](#)
[View Session History](#)
[New Search](#)
[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((bilinear &lt;and&gt; authorities)&lt;in&gt;metadata)

☐ Check to search only within this results set

Display Format:



Citation



Citation &amp; Abstract

IEEE/ET

Books

Educational Courses

IEEE/ET journals, transactions, letters, magazines, conference proceedings, and standards.

[Select All](#) [Deselect All](#)

1. Cryptanalysis and Improvement of a Certificateless Proxy Signature Scheme from Bilinear Lu, Rongbo; He, Dake; Wang, Changji; [Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. International Conference on](#)  
Volume 3, July 30 2007-Aug. 1 2007 Page(s):285 - 290  
Digital Object Identifier 10.1109/SNPD.2007.220  
[AbstractPlus](#) | Full Text: [PDF\(402 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
2. Multi-Dimensional Range Query over Encrypted Data Shi, Elaine; Bethencourt, John; Chan, T-H. Hubert; Song, Dawn; Perrig, Adrian; [Security and Privacy, 2007. SP '07. IEEE Symposium on](#)  
20-23 May 2007 Page(s):350 - 364  
Digital Object Identifier 10.1109/SP.2007.29  
[AbstractPlus](#) | Full Text: [PDF\(309 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
3. An efficient secure key issuing protocol in ID-based cryptosystems Gangishetti, R.; Gorantla, M.C.; Das, M.L.; Saxena, A.; Gulati, V.P.; [Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on](#)  
Volume 1, 4-6 April 2005 Page(s):674 - 678 Vol. 1  
Digital Object Identifier 10.1109/ITCC.2005.75  
[AbstractPlus](#) | Full Text: [PDF\(112 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
4. On the Security of an Identity-Based Threshold Proxy Signature Scheme with Known Signer Lu, Rongbo; He, Dake; Wang, Changji; [Natural Computation, 2007. ICNC 2007. Third International Conference on](#)  
Volume 3, 24-27 Aug. 2007 Page(s):210 - 214  
Digital Object Identifier 10.1109/ICNC.2007.515  
[AbstractPlus](#) | Full Text: [PDF\(267 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
5. A path-following method for solving BMI problems in control

Hassibi, A.; How, J.; Boyd, S.;  
[American Control Conference, 1999. Proceedings of the 1999](#)  
Volume 2, 2-4 June 1999 Page(s):1385 - 1389 vol.2  
Digital Object Identifier 10.1109/ACC.1999.783595  
[AbstractPlus](#) | [Full Text: PDF\(432 KB\)](#) | [IEEE CNF](#)  
[Rights and Permissions](#)

[Help](#) [Contact](#)

[© Copy](#)

